EXHIBIT 2

STATUTORY AUTHORITY

1. This investigation concerns alleged violations of 18 U.S.C. § 2252A, relating to material involving the sexual exploitation of minors.

2. 18 U.S.C. § 2252A(a)(2) prohibits knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

3. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer.

PROBABLE CAUSE

4. On XX/XX/XXXX, your Affiant conducted an online Internet investigation to identify those possessing and sharing child pornography on the internet using a Peer to Peer network (P2P). P2P networks facilitate the trading of files by multiple users through one network. Users must elect to download software or a client to operate on a specific P2P network. There are multiple P2P is a P2P network used to exchange files between computers. Your Affiant was utilizing a P2P network that uses file hashing to uniquely identify files on the network.

5. Using the above described client software program, your Affiant identified a computer with the IP address XXX.XXX.XX.XX that made available for sharing at least 37 files of investigative interest. Files of investigative interest are files previously identified by law enforcement as child pornography whose hash values are input into the program to alert law enforcement to the trafficking of those images. When an investigator observes a user on the network sharing files of investigative interest, the investigator can focus their investigation on one user. Your Affiant used a Peer to Peer (P2P) file sharing program that downloads only from one source at a time to facilitate this.

6. Even though the P2P network links together computers from all over the world and users can download files, it is not possible for one user to send or upload a file to another user of the P2P network. The software is specifically designed only to allow files to be downloaded that have been selected. A user does not have the ability to send files from his/her computer to another user's computer without their permission or knowledge. Therefore, it is not possible for one user to send or upload child pornography files to another user's computer without his/her active participation. Your Affaint therefore, is only able to download files another user on the network has elected to share.

7. During the investigation the P2P client program on the computer with the IP address XXXXXXX, reported its version as XXXXX. This client program reported its nickname as: XXX@XXX.

8. On XX/XX/XXXX, your Affiant downloaded files made available for sharing by the user of IP address XX.XX.XXX.XXX. Your Affiant downloaded a total of XX files, XX of which were image files and XX of which were video files.

9. On XX/XX/XXXX, your Affiant reviewed the files downloaded from the user of IP address XX.XX.XX.XXX. Of the XXX files downloaded, XX files depicted children engaged in sexually explicit conduct. The following are three of those files:

FILE TITLE.jpg: an image file that depicts a prepubescent

FILE TITLE.jpg: an image file that depicts a prepubescent

FILE TITLE.jpg: an image file that depicts a prepubescent

10. On XX/XX/XXXX, your Affiant conducted a query of publicly available records located online by an organization known as the American Registry of Internet Numbers and determined that IP address XX.XX.XXX.XXX was assigned to the Internet Service Provider XXXXX.

11. On XX/XX/XXXX, your Affiant faxed an administrative subpoena to XXX requesting basic subscriber information for IP address XXX.XX.XXX on XX/XX/XXXX.

12. On XX/XX/XXXX, XXXX provided the results from the administrative subpoena. The account information for the subscriber of the IP address XX.XX.XX on XX/XX/XXXX is:

CONCLUSION

13. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B which are in violation of 18 U.S.C. § 2252A.

Respectfully submitted,

Special Agent
United States Secret Service

Subscribed and sworn to before me
on June 13, 2016:

_____
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Location to be Searched

The property to be searched is the residence, property, and curtilage, located at

ATTACHMENT B

Property to be Seized

1. All records relating to violations of 18 U.S.C. § 2252A, including:

   a. Records and information relating to communications with Internet Protocol address XX.XXX.XXXX.

   b. Records and information relating to malicious software;

2. Computers or storage media used as a means to commit the violations described above, including possessing or distributing child pornography in violation of 18 U.S.C. § 2252A.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

   a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

   b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

   c. evidence of the lack of such malicious software;

   d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

   e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, software that the user would use to access a P2P network;

k. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.